The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/29/2016

SUBJECT:
Multiple Vulnerabilities in PHP Could Allow For Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in PHP, the most severe of which could allow an attacker to execute arbitrary code, with failed exploit attempts potentially leading to denial of service conditions. PHP is a programming language originally designed for use in web-based applications with HTML content. PHP supports a wide variety of platforms and is used by numerous web-based software applications. Successfully exploiting these issues could allow remote attackers to execute arbitrary code in the context of the affected application.

THREAT INTELLIGENCE:
The following exploit is available:
Hans Jerry Illikainen 2016-04-28 00:00:00Z
hxxp://downloads.securityfocus[.]com/vulnerabilities/exploits/88765.py

SYSTEM AFFECTED:
- PHP 7 prior to 7.0.6
- PHP 5 prior to 5.5.35
- PHP 5 prior to 5.6.21

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
PHP has released updates that address multiple vulnerabilities, the most severe of which could allow for arbitrary code execution. These vulnerabilities include:

Prior to 5.5.35 and 5.6.21

- Fixed bug #71912 (libgd: signedness vulnerability) (CVE-2016-3074)

Prior to 7.0.6

- Fixed bug #71912 (libgd: signedness vulnerability) (CVE-2016-3074)
- Fixed bug #71923 (integer overflow in ZipArchive::getFrom*) (CVE-2016-3078)

Successful exploitation of these vulnerabilities may allow remote attackers to execute arbitrary code in the context of the webserver. Other bugs fixed in the PHP Core for these versions may be found below:

- Fixed bug #71930 (_zval_dtor_func: Assertion `(arr)->gc.refcount <= 1' failed).
- Fixed bug #71922 (Crash on assert(new class{})).
- Fixed bug #71914 (Reference is lost in "switch").
- Fixed bug #71871 (Interfaces allow final and abstract functions).
- Fixed bug #71859 (zend_objects_store_call_destructors operates on realloced memory, crashing).
- Fixed bug #71841 (EG(error_zval) is not handled well).
- Fixed bug #71750 (Multiple Heap Overflows in php_raw_url_encode/ php_url_encode).
- Fixed bug #71731 (Null coalescing operator and ArrayAccess).
- Fixed bug #71609 (Segmentation fault on ZTS with gethostbyname).
- Fixed bug #71428 (inheritance and allow_null).
- Fixed bug #71414 (Inheritance, traits and interfaces).
- Fixed bug #71359 (Null coalescing operator and magic).
- Fixed bug #71334 (Cannot access array keys while uksort()).
- Fixed bug #69659 (ArrayAccess, isset() and the offsetExists method).
- Fixed bug #69537 (__debugInfo with empty string for key gives error).
- Fixed bug #62059 (ArrayObject and isset are not friends).
- Fixed bug #71980 (Decorated/Nested Generator is Uncloseable in Finally).
- Fixed bug #72093 (bcpowmod accepts negative scale and corrupts _one_ definition).
- Fixed bug #71831 (CURLOPT_NOPROXY applied as long instead of string).
- Fixed bug #71889 (DateInterval::format Segmentation fault).
- Fixed bug #72094 (Out of bounds heap read access in exif header processing).
- Fixed bug #71516 (IntlDateFormatter looses locale if pattern is set via constructor).
- Fixed bug #70455 (Missing constant: IntlChar::NO_NUMERIC_VALUE).
- Fixed bug #70451, #70452 (Inconsistencies in return values of IntlChar methods).
- Fixed bug #68893 (Stackoverflow in datefmt_create).
- Fixed bug #66289 (Locale::lookup incorrectly returns en or en_US if locale is empty).
- Fixed bug #70484 (selectordinal doesn't work with named parameters).
- Fixed bug #72061 (Out-of-bounds reads in zif_grapheme_stripos with negative offset).
- Fixed bug #63171 (Script hangs after max_execution_time).
- Fixed bug #71843 (null ptr deref ZEND_RETURN_SPEC_CONST_HANDLER).
- Fixed bug #52098 (Own PDOStatement implementation ignore __call()).
- Fixed bug #71447 (Quotes inside comments not properly handled).
- Fixed bug #71943 (dblib_handle_quoter needs to allocate an extra byte).
- Add DBLIB-specific attributes for controlling timeouts.
- Fixed bug #62498 (pdo_pgsql inefficient when getColumnMeta() is used).
- Fixed bug #71820 (pg_fetch_object binds parameters before call constructor).
- Fixed bug #71998 (Function pg_insert does not insert when column type = inet).
- Fixed bug #71986 (Nested foreach assign-by-reference creates broken variables).

- Fixed bug #71838 (Deserializing serialized SPLObjectStorage-Object can't access properties in PHP).
- Fixed bug #71735 (Double-free in SplDoublyLinkedList::offsetSet).
- Fixed bug #67582 (Cloned SplObjectStorage with overwritten getHash fails offsetExists()).
- Fixed bug #52339 (SPL autoloader breaks class_exists()).
- Fixed bug #72116 (array_fill optimization breaks implementation).
- Fixed bug #71995 (Returning the same var twice from __sleep() produces broken serialized data).
- Fixed bug #71940 (Unserialize crushes on restore object reference).
- Fixed bug #71969 (str_replace returns an incorrect resulting array after a foreach by reference).
- Fixed bug #71891 (header_register_callback() and register_shutdown_function()).
- Fixed bug #71884 (Null pointer deref (segfault) in stream_context_get_default).
- Fixed bug #71840 (Unserialize accepts wrongly data).
- Fixed bug #71837 (Wrong arrays behaviour).
- Fixed bug #71827 (substr_replace bug, string length).
- Fixed bug #67512 (php_crypt() crashes if crypt_r() does not exist or _REENTRANT is not defined).
- Fixed bug #72099 (xml_parse_into_struct segmentation fault).

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade to the latest version of PHP immediately, after appropriate testing.
- Apply the principle of Least Privilege to all systems and services.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.
- Limit user account privileges to only those required.

REFERENCES:

PHP:

NOTE: Visiting these links may trigger an IDS signature match for a Possible Encrypted Webshell Download. This is a false positive alert that is matching content on the pages below.

https://secure.php.net/index.php#id2016-04-29-1
http://php.net/ChangeLog-7.php#7.0.6
http://php.net/ChangeLog-5.php#5.6.21
http://php.net/ChangeLog-5.php#5.5.35

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3078
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3074